REMARKS

In view of the above amendment and the following discussion, the Applicant submits that none of the claims now pending in the application is unpatentable under the provision of 35 U.S.C. §102 or 35 U.S.C. §103. Thus, the Applicant believes that all of these claims are now in allowable form.

I. OBJECTIONS TO CLAIMS 5 AND 13

The Examiner has objected to claims 5 and 13 due to informalities. In particular, the Examiner noted that the claims have incorrect punctuation.

In response, the Applicant has amended claims 5 and 13 to correct the typographical errors. As such, the Applicant respectfully requests that the objection be withdrawn.

II. REJECTION OF CLAIMS 1, 5, 9, AND 13 UNDER 35 U.S.C. § 102

The Examiner has rejected claims 1, 5, 9, and 13 in the Office Action under 35 U.S.C. §102 as being anticipated by the Bailey, III reference (U.S. Patent 5,659,614, issued August 19, 1997, hereinafter referred to as "Bailey"). The Applicant respectfully traverses the rejection.

Bailey teaches a method and system for creating and storing a backup copy of file data stored on a computer. "The file data to be backed up is encrypted using multiple, indirect encryption keys, variable block lengths, and variable algorithms based on a client-selected string of characters. The files are thereafter encrypted again at the client site prior to transmission to the backup site. A program registry is maintained at the backup site that contains a master copy of many commercially-available files. The incoming files received from the client site are compared to the files in the program registry. If an incoming file is located in the registry, the file is replaced by a token identifying the commercially-available file and the token is stored at the backup facility" (see Bailey, Abstract).

Page 5

The Examiner's attention is directed to the fact that Bailey fails to teach or suggest the novel concept of <u>generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle</u>, as positively claimed by the Applicant in claims 1 and 9. In addition, the Applicant submits that Bailey fails to teach or suggest the <u>checking for an authentication code in the compressed bundle</u>, as positively claimed by the Applicant in claims 5 and 13. Specifically, Applicant's independent claims 1, 5, 9, and 13 positively recite:

1.   A method of backing up one or more files on a local device onto remote servers over a network comprising:
    deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
    compressing one or more files and adding each of the files to a bundle;
    <u>generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle</u>; and
    encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added)

5.   A method of restoring one or more files on remote servers to a local device over a network comprising:
    deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
    decrypting a bundle received from the remote server using the second cryptographic key;
    <u>checking an authentication code in the bundle</u> using the first cryptographic key; and
    decompressing one or more files from the bundle. (Emphasis added)

9.   A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
    deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
    compressing one or more files and adding each of the files to a bundle;
    <u>generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle</u>; and
    encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added)

13.   A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
    deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
    decrypting a bundle received from the remote server using the second cryptographic key;
    checking <u>an authentication code in the bundle</u> using the first cryptographic key; and
    decompressing one or more files from the bundle. (Emphasis added)

Page 6

The Applicant's invention provides a method and device-readable medium storing program instructions for backing up files on a local device onto remote servers over a network (see claims 1 and 9). More specifically, the invention prompts for a user-provided passphrase that is used to derive two cryptographic keys. An authentication code for a bundle (i.e., compressed data) is generated using the first of the two cryptographic keys. The authentication code is then added to the bundle, which is subsequently encrypted using the second cryptographic key. Lastly, the encrypted bundle is sent to the remote server to complete the backup process.

Likewise, the Applicant's invention provides a method and device-readable medium storing program instructions for restoring files on remote servers to a local device over a network (see claims 5 and 13). The restoring process is similar to the backup process described above except it is executed in reverse order.

Bailey fails to teach or suggest a method that entails the generation of an authentication code that is added to a bundle of compressed data and subsequently encrypted as a whole with the data bundle. The Examiner alleged that Bailey teaches this concept by citing column 17, line 1 to column 19, line 5. However, Bailey teaches an encryption method that utilizes ASCII conversion and a random number set. Bailey also teaches a two level encryption, i.e., the data is encrypted using a first key and then followed by encryption of the encrypted data using a second key. This multilevel encryption is not Applicant's invention and is computationally expensive. Applicant's first key is only used to generate the authentication code and it is not used to encrypt the compressed data. Furthermore, Bailey does not teach or even mention the generation of an authorization code, much less a code that is added to and encrypted along with a bundle.

Therefore, the Applicant respectfully submits that independent claims 1, 5, 9, and 13 are patentable and not anticipated by Bailey. As such, the Applicant respectfully requests the rejection be withdrawn.

III. REJECTION OF CLAIMS 2-4, 6-8, 10-12, AND 14-16 UNDER 35 U.S.C. §103

The Examiner has rejected claims 2-4, 6-8, 10-12, and 14-16 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of the Walmsley

reference (U.S. Publication No. 2004/0049468, published March 11, 2004, hereinafter referred to as "Walmsley"). The Applicant respectfully traverses the rejection.

Bailey has been discussed above.

Walmsley teaches "a consumable authentication method for validating the existence of an untrusted chip. A random number is encrypted using a first key and sent to an untrusted chip. In the untrusted chip it is decrypted using a secret key and re-encrypted together with a data message read from the untrusted chip. This is decrypted so that a comparison can be with the generated random number and the read data message" (see Walmsley, Abstract).

The Applicant submits that Walmsley does not bridge the substantial gap existing between the Applicant's invention and Bailey. More specifically, the Applicant contends that Walmsley does not teach, suggest, or mention an authentication code as set forth in claims 1, 5, 9, and 13. The Examiner's attention is directed to the fact that Bailey in view of Walmsley fails to disclose or suggest the novel concept of generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle as claimed in Applicant's independent claims 1 and 9 from which claims 2-4 and 10-12 depend. Similarly, Bailey in view of Walmsley fails to disclose or suggest the novel concept of checking an authentication code that was encrypted in the bundle using a first cryptographic key as claimed in Applicant's independent claims 5 and 13 from which claims 6-8 and 14-16 depend.

Consequently, the Applicant submits that claims 1, 5, 9, and 13 would not be made obvious by the teaching of Bailey in view of Walmsley, and therefore, are patentable under 35 U.S.C. §103.

Since claims 2-4, 6-8, 10-12, and 14-16 depend, either directly or indirectly, from claims 1, 5, 9, and 13, and recite additional features thereof, the Applicant submits that claims 2-4, 6-8, 10-12, and 14-16 are also not made obvious by the teaching of Martinez. Therefore, the Applicant submits that claims 2-4, 6-8, 10-12, and 14-16 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.
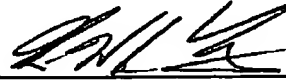
Conclusion

Thus, the Applicant submits that all of these claims now fully satisfy the requirement of 35 U.S.C. §102 and §103. Consequently, the Applicant believes that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone <u>Mr. Kin-Wah Tong, Esq.</u> at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

12/2/04

Moser, Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Page 9